(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 2001273211 A

(43) Date of publication of application: 05.10.01

(51) Int. Cl G06F 13/00
H04L 12/22
H04L 12/24
H04L 12/56
H04L 12/58

(21) Application number: 2001037593

(22) Date of filing: 14.02.01

(30) Priority: 15.02.00 US 2000 504157

(71) Applicant: HEWLETT PACKARD CO <HP>

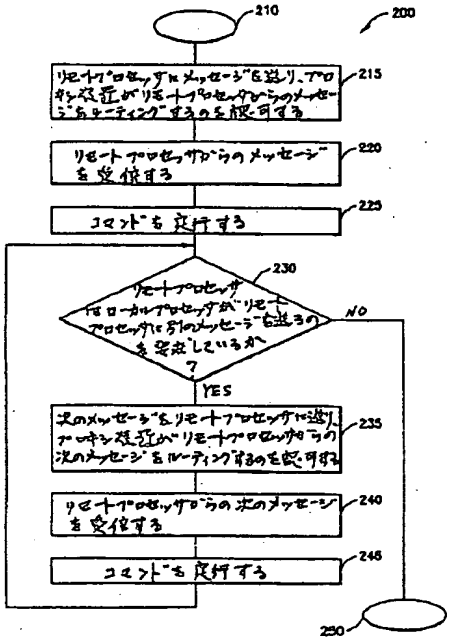
(72) Inventor: SIT ERIC N
CLOUGH JAMES
NELSON DEAN S

(54) METHOD AND DEVICE FOR CONTROLLING DEVICE INSIDE FIREWALL FROM OUTSIDE

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a method for enabling a remote processor to communicate with a local processor through a computer network and a firewall.

SOLUTION: The remote processor is connected to the local processor through a reverse proxy device, the computer network, the firewall and a proxy agent device. By dispatching a local request message to the proxy agent device, the local processor establishes a communication channel with the remote processor. The proxy agent device makes a response received from the local processor seem like a request and converts a response received from the firewall into a request. Similarly, the reverse proxy device converts a request received from the firewall into a response and makes a request received from the remote processor seem like a response.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－273211
（P2001－273211A）
(43)公開日　平成13年10月5日(2001.10.5)

(51)Int.Cl.⁷		識別記号	FI		テーマコード（参考）
G06F	13/00	351	G06F	13/00	351Z
H04L	12/22		H04L	12/22	
	12/24			12/24	
	12/56			12/56	A
	12/58	100		12/58	100A

審査請求　未請求　請求項の数1　ＯＬ　（全 11 頁）

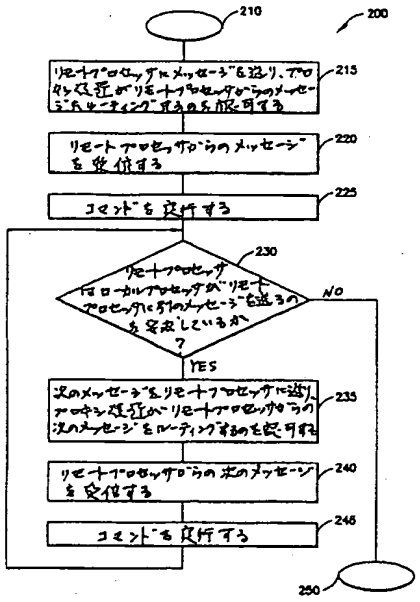
(21)出願番号　特願2001－37593(P2001－37593)
(22)出願日　平成13年２月14日(2001.2.14)
(31)優先権主張番号　５０４１５７
(32)優先日　平成12年２月15日(2000.2.15)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　398038580
ヒューレット・パッカード・カンパニー
HEWLETT－PACKARD COMPANY
アメリカ合衆国カリフォルニア州パロアルト　ハノーバー・ストリート　3000
(72)発明者　エリック・エヌ・シット
アメリカ合衆国ニュージャージー州ウァッチュング　クレストウッド・ドライブ　115
(74)代理人　100078053
弁理士　上野　英夫

最終頁に続く

(54)【発明の名称】　ファイヤウォール内部の装置を外部から制御する方法及び装置

(57)【要約】
【課題】リモートプロセッサが、コンピュータネットワークとファイヤウォールとを介して、ローカルプロセッサと通信できるようにする方法を提供する。
【解決手段】本発明の一実施例によれば、リモートプロセッサは、リバースプロキシ装置と、コンピュータネットワークと、ファイヤウォールと、プロキシエージェント装置とを介してローカルプロセッサに結合される。ローカルプロセッサは、プロキシエージェント装置にローカル要求メッセージをディスパッチすることにより、リモートプロセッサとの通信チャネルを確立する。プロキシエージェント装置はローカルプロセッサから受信した応答を要求のように見せるとともに、ファイヤウォールから受信した応答を要求に変換する。同様に、リバースプロキシ装置は、ファイヤウォールから受信した要求を応答に変換するとともに、リモートプロセッサから受信した要求を応答のように見せる。



1

【特許請求の範囲】

【請求項１】リモートプロセッサが、リバースプロキシ装置と、コンピュータネットワークと、ファイヤウォールと、プロキシエージェント装置とを介してローカルプロセッサに結合される場合に、前記リモートプロセッサが前記ローカルプロセッサと通信できるようにするトンネリング動作を可能にするための方法であって、

ローカル要求メッセージを前記プロキシエージェント装置にディスパッチさせて前記リモートプロセッサとの通信チャネルを確立するよう、前記ローカルプロセッサを制御するステップであって、前記プロキシエージェント装置は前記ファイヤウォールと前記ネットワークとを介して前記ローカル要求メッセージを前記リバースプロキシ装置にディスパッチし、前記ファイヤウォールは前記プロキシエージェント装置によって前記ローカル要求メッセージに対するリモート応答メッセージを受信することができるようになされる、制御ステップと、

前記通信チャネルの確立に基づき、前記リモートプロセッサが前記リバースプロキシ装置にリモート要求メッセージを送出するのを可能にし、次に、前記リバースプロキシ装置が、前記リモート要求メッセージを中に含んだリモート応答メッセージをディスパッチするのを可能にするステップと、

前記ファイヤウォールを介して前記プロキシエージェント装置が前記リモート応答メッセージを受信したときに、前記リモート要求メッセージを抽出して該リモート要求メッセージを前記ローカルプロセッサにディスパッチするよう前記プロキシエージェント装置を制御するステップと、

を備えて成り、前記プロキシエージェント装置及び前記リバースプロキシ装置が、前記ローカルプロセッサまたは前記リモートプロセッサのいずれかにおける通信アプリケーションを変更することなく、前記トンネリング動作を可能にすることを特徴とする方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ファイヤウォールを通過するメッセージ転送に関し、より詳細には、ファイヤウォールによって保護される装置が、ファイヤウォールの外部にある装置によって制御できるようにする方法に関する。

【０００２】

【従来の技術】多くの場合、コンピュータデータ処理システムは、ローカル・エリア・ネットワーク（ＬＡＮ）内で、プロセッサ或いはサーバに接続される、プリンタのような一群の周辺機器を備える。プロセッサ上で動作するソフトウエアによって、利用者は、動作パラメータを構成し、ローカルに接続される全ての周辺機器の動作をモニタすることが可能になる。

【０００３】一般に、コンピュータシステムによって提

2

供される特徴及び利便性が向上するのに応じて、システムを制御するソフトウエアは益々精巧で、複雑になる。システムのインストール及びトラブルシューティングは、システム及び周辺機器の専門知識を必要とする場合が多い。問題を突き止める場合、システムの利用者は、この専門知識を持つ技術サポートエンジニアから支援を受けなければならない。

【０００４】利用者が最初に支援を求めるのは、典型的にはサービスセンタに電話することであり、技術サポート担当者と話をすることである。担当者は最初に、問題になっている特定のシステムの構成に関して、利用者から情報を聴取し、その後インストール及びトラブルシューティング手順を通して、利用者を誘導する。

【０００５】電話による技術サポートは、大抵の場合に時間と費用がかかる。また利用者及び技術担当者のいずれにおいてもリソースを必要とし、長距離電話による通話を伴う場合もある。成功させるためには、利用者及び担当者は、長時間の会話をし続け、技術情報及び指示を交換できなければならない。この解決は、会話による疎通がうまくいかなかったり、或いは利用者及び担当者が十分な訓練を受けていないことによって間違いが起こりやすい。最も良好な場合であっても、成功する保証はない。電話による技術サポートのやり取りが失敗すれば、利用者には、不快感から完全な失望感までの様々な感情が残り、サポートを提供する企業のイメージを損なう恐れもある。

【０００６】担当者が最初に問題のシステムにアクセスしている場合には、技術サービスは改善される。これは、そのシステムが設置されている場所に移動することによりなし得るが、必然的にその場所への行き来に費用がかかる。好ましい別の形態では、担当者がそのシステムにリモートアクセスすることである。

【０００７】インターネットは、遠隔して位置するコンピュータが互いに情報を交換することができるチャネルを提供する。第１のコンピュータが、インターネット内で情報の要求を、第２のコンピュータに送出することができる。その後、第２のコンピュータは、所望の情報を含むメッセージで応答する。

【０００８】セキュリティ及びシステムの保全性のため、多くの組織は、その組織の外部にあるコンピュータとの情報の交換を制限するファイヤウォールを導入している。ファイヤウォールは、不要な受信要求及び情報を遮断するために、ローカルコンピュータシステムとインターネットとの間に介在する。その結果、ファイヤウォールによって保護されるローカルコンピュータシステムに、遠隔した場所から無条件にアクセスすることはできない。

【０００９】図１を参照すると、ローカルコンピュータ５０とリモートコンピュータ７０がインターネット６５を介して接続される。プロキシ装置６０は、ローカルコ

ンピュータ５０とインターネット６５との間に介在し、動作する。

【００１０】プロキシ装置６０は、ローカルコンピュータ５０に代わってインターネット６５とのインターフェースを形成し、認可を受けた場合にのみ、メッセージをインターネット６５からローカルコンピュータ５０にルーティングする。例として、ローカルコンピュータ５０が、プロキシ装置６０を介して、リモートコンピュータ７０に要求７５を送出することにより、リモートコンピュータ７０との通信を開始する。要求７５は、プロキシ装置６０がリモートコンピュータ７０からローカルコンピュータ５０にメッセージをルーティングするのを認可する、ハイパーテキスト転送プロトコル（ＨＴＴＰ）ヘッダ内のプロキシ情報を含む。その後、リモートコンピュータ７０が応答８０を送出し、プロキシ装置６０がその応答８０をローカルコンピュータ５０にルーティングする。

【００１１】プロキシ装置６０は、認可されていないメッセージがインターネット６５からローカルコンピュータ５０にルーティングされるのを防ぐことによって、ローカルコンピュータ５０の保全性を保護するためのファイヤウォールとして機能する。プロキシ装置６０は認可されていない受信情報を遮断するだけでなく、遮断しなければローカルコンピュータ５０が応答してしまうような、認可を受けずに受信した要求も遮断する。従って、リモートコンピュータ７０は、無条件には、ローカルコンピュータ５０との間でデータを読み書きすることができない。

【００１２】ローカルコンピュータ５０は、プロキシ装置６０が受信メッセージを受け取るのをメッセージ毎に認可しなければならないため、リモートコンピュータ７０からローカルコンピュータ５０への各メッセージは、ローカルコンピュータ５０によって開始されなければならない。いくつかのメッセージが交換される状況では、要求及び応答のパターンが必要とされる。ローカルコンピュータ５０は要求７５を送出し、応答７６を受信し、要求７７を送出し、応答７８を受信し、要求７９を送出し、応答８０を受信する、というようなパターンが続く。一般的な場合には、ローカルコンピュータ５０は、リモートコンピュータ７０への要求を送出し、リモートコンピュータ７０から応答を受信する。

【００１３】技術サポート担当者が、遠隔して配置されているコンピュータシステムを管理したい場合がある。リモートアクセスを通して、担当者は、システムサイトの利用者の側からほとんど、或いは全く介入することなく、システムを構成し、モニタし、トラブルシューティングすることができる。さらに、担当者には、そのコンピュータシステムへの担当者のアクセスを制限するファイヤウォールによって保護されているコンピュータシステムにアクセスする必要がある場合もある。

【００１４】【発明が解決しようとする課題】本発明の目的は、リモートコンピュータシステムが、インターネットを介して、ファイヤウォールがインターネットとローカルコンピュータシステムの間に介在して動作するローカルコンピュータシステムにアクセスするための方法を提供する。

【００１５】本発明の別の目的は、リモートコンピュータシステムが、インターネットを介してローカルコンピュータシステムに通信するための方法を提供し、その方法では、インターネットとローカルコンピュータシステムとの間に介在して動作し、ローカルコンピュータシステム或いはリモートコンピュータシステムのいずれかにおいて動作するアプリケーションを変更する必要がない制御機能を付与することにより、そのような通信を制御する。

【００１６】【課題を解決するための手段】本発明は、リモートプロセッサが、リバースプロキシ装置と、コンピュータネットワークと、ファイヤウォール装置と、プロキシエージェント装置とを介して、ローカルプロセッサに接続される場合に、リモートプロセッサがローカルプロセッサと通信できるようにするトンネリング動作を可能にする。最初に、ローカルプロセッサは、プロキシエージェント装置にローカル要求メッセージをディスパッチすることにより、リモートプロセッサとの通信チャネルを確立する。プロキシエージェント装置は、ファイヤウォール及びネットワークを介してローカル要求メッセージをリバースプロキシ装置にディスパッチし、それにより、ファイヤウォールが、そのローカル要求メッセージへのリモート応答メッセージを受信できるようにする。その後、リモートプロセッサはリモート要求メッセージをリバースプロキシ装置に送り、次にリバースプロキシ装置はリモート要求メッセージを中に含んだリモート応答メッセージを、ファイヤウォールにディスパッチする。（ファイヤウォールを介して）リモート応答メッセージがプロキシエージェント装置よって受信されると、プロキシエージェント装置は、ローカルプロセッサへのリモート要求メッセージを抽出し、ディスパッチする。ローカルプロセッサによるローカル応答メッセージのディスパッチによって、プロキシエージェントは、ローカル応答メッセージをローカル要求メッセージに組み込み、ファイヤウォール及びリバースプロキシ装置を介して、リモートプロセッサにローカル要求メッセージをディスパッチできるようになる。

【００１７】【発明の実施の形態】従来からのインターネット用語において、かつハイパーテキスト転送プロトコル（ＨＴＴＰ）に従えば、「要求」は、第２のプロセッサからの情報を求める第１のプロセッサによって発行されるメッセ

ージであり、「応答」は、要求された情報を含む、第２のプロセッサから第１のプロセッサへのメッセージである。通常、ファイヤウォールの後ろで保護されて、プロセッサは要求を発行し、応答を受信する。本発明では、ローカルプロセッサはリモートプロセッサへの第１の要求を行うが、その後、リモートプロセッサからのメッセージは「要求」になり、リモートプロセッサへのメッセージは「応答」になる。こうして、ファイヤウォール外部の装置管理を行うためのリバース（逆）ＨＴＴＰ接続が確立される。

【００１８】図２は、特に本発明を実行するように構成されたコンピュータシステムのブロック図である。一群の周辺機器１１０が、ＬＡＮ１１２内のローカルプロセッサ１２２に接続される。ローカルコンピュータ１２０は、プロキシ装置１４５を介してインターネット１５０に接続される。リモートコンピュータ１５５もインターネット１５０に接続される。

【００１９】ローカルコンピュータ１２０は、ローカルプロセッサ１２２と、コンピュータメモリ（図示せず）と、クライアント装置管理ゲートウエイ（ＣＤＭＧ）１２５とを備える。ＣＤＭＧ１２５は、ローカルプロセッサ１２２を制御して、本発明の方法を実行する。リモートコンピュータ１５５は、リモートプロセッサ１５７と、装置１１０を制御するためにＣＤＭＧ１２５と通信を行うサポートアプリケーション１６０とを備える。

【００２０】ＣＤＭＧ１２５は、ローカルプロセッサ１２２を制御して、プロキシ装置１４５を介してリモートプロセッサ１５７に要求１７０を送出することにより、リモートプロセッサ１５７との通信を開始する。要求１７０は典型的には、ローカルプロセッサ１２２と装置１１０とを識別する情報を含むであろう。要求１７０はまた、プロキシ装置１４５がリモートプロセッサ１５７からローカルプロセッサ１２２にメッセージをルーティングするのを認可するＨＴＴＰヘッダのプロキシ情報も含む。その後、リモートプロセッサ１５７は、プロキシ装置１４５がローカルプロセッサ１２２にルーティングする要求１７１を送出することにより応答する。要求１７１は、要求１７０への有効な応答であることに留意されたい。

【００２１】要求１７１は、装置１１０に対してローカルプロセッサ１２２によって実行されることになる１つ或いは複数のコマンドを指示するメッセージである。例えば、コマンドは、装置１１０が再度初期化されるべきであることを示すことができる。また要求１７１は、リモートプロセッサ１５７に情報を送出するように、ローカルプロセッサ１２２を指示することができる。例えば、サポートアプリケーション１６０は、ローカルプロセッサ１２２或いは装置１１０の構成に関する付加情報を必要とする場合もある。ローカルプロセッサ１２２は、応答１７２において要求された情報を送出する。

【００２２】応答１７２は、プロキシ装置１４５がリモートプロセッサ１５７からローカルプロセッサ１２２に、別の「応答」メッセージをルーティングするのを認可するＨＴＴＰヘッダのプロキシ情報を含む。その後、リモートプロセッサ１５７は、プロキシ装置１４５がローカルプロセッサ１２２にルーティングする要求１７３を送出する。要求１７３は、装置１１０に対して実行されるべきコマンドを指示することができ、リモートプロセッサ１５７にさらに情報を与えるためにローカルプロセッサ１２２を指示することもできる。要求１７３が、ローカルプロセッサ１２２が付加情報を送出するよう指示する指示を含む場合には、ローカルコンピュータは応答１７４において付加情報を送出する。

【００２３】要求１７０が送出された後、要求及び応答のパターンが明らかになることに留意されたい。一般的な場合には、リモートプロセッサ１５７はローカルプロセッサ１２２に要求を送出し、ローカルプロセッサ１２２から応答を受信する。このパターンは、図１に示されるパターンの反対である。ローカルプロセッサ１２２によってリモートプロセッサ１５７に送出される各メッセージ（要求１７０及び応答１７２、１７４）は、プロキシ装置１４５がリモートプロセッサ１５７からローカルプロセッサ１２２にメッセージ（要求１７１、１７３）をルーティングするのを認可するＨＴＴＰヘッダのプロキシ情報を含む。それによって装置１１０は、リモートプロセッサ１５７によって間接的に制御される。

【００２４】ＣＤＭＧ１２５は、キーボードのような任意の標準的なユーザインターフェースを介して適用される通信開始コマンド１３０に応答して、リモートプロセッサ１５７との通信を開始するであろう。これは例えば、ローカルプロセッサ１２２の利用者が、装置１１０をインストール或いはトラブルシューティングする支援を必要とする場合に相当するであろう。

【００２５】またＣＤＭＧ１２５は、電子メール（Ｅメール）を介して受信した通信開始コマンド１４０に応答して通信を開始するであろう。簡易メール転送プロトコル（ＳＭＴＰ）を用いて、リモートプロセッサ１５７は、通信開始要求１６５ＡとしてＥメールサーバ１３５に格納される通信開始要求１６５を送出することができる。通信開始要求１６５（及び１６５Ａ）は、通信開始コマンド１４０を含む。通信開始コマンド１４０は、Ｅメールサーバ１３５を定期的にポーリングするＣＤＭＧ１２５によって、通信開始要求１６５ＡがＥメールサーバ１３５から読み出される際に実行される。通信開始要求１６５は、例えば、装置１１０の性能が、サポートアプリケーション１６０によって定期的に評価、かつ較正される場合に用いることができる。また第三者（図示せず）が装置１１０を自動的にモニタし、較正するための機会を与えることができる。

【００２６】ＣＤＭＧ１２５を起動して通信を開始する

ための第３の方法は、装置１１０Ａ内からの通信開始コマンド１１３によって生成可能である。通信開始コマンド１１３は、セルフテストを通して自動的に実行し、異常を検出するか、或いは定期的にメンテナンスプログラムを実行する場合に用いられる。装置１１０Ａは、通信開始コマンド１１３をＣＤＭＧ１２５に発行し、その後ＣＤＭＧ１２５は、リモートプロセッサ１５７との通信を開始し、装置１１０Ａの自動テスト及び較正を開始する。

【００２７】図３は、本発明を実行するためのコンピュータシステムの別の実施形態のブロック図である。装置１１０ｂは、プロキシ装置１４５を介してインターネット１５０に接続される。リモートコンピュータ１５５もインターネット１５０に接続される。

【００２８】装置１１０ｂは、ローカルプロセッサ１２２Ａと、コンピュータメモリ（図示せず）と、クライアント装置管理ゲートウエイ（ＣＤＭＧ）１２５Ａとを備える。ＣＤＭＧ１２５Ａは、ローカルプロセッサ１２２Ａを制御して、本発明の方法を実行する。リモートコンピュータ１５５は、リモートプロセッサ１５７と、装置１１０ｂを制御するためにＣＤＭＧ１２５Ａと通信を行うサポートアプリケーション１６０とを備える。

【００２９】通信開始コマンド１１３Ａは、装置１１０ｂがセルフテストを通して自動的に実行し、異常を検出するか、或いは定期的にメンテナンスプログラムを実行する場合に生成される。通信開始コマンド１１３Ａは、ＣＤＭＧ１２５を起動し、リモートプロセッサ１５７との通信を開始する。

【００３０】ＣＤＭＧ１２５Ａはローカルプロセッサ１２２Ａを制御して、プロキシ装置１４５を介してリモートプロセッサ１５７に要求１７０を送出することにより、リモートプロセッサ１５７との通信を開始する。要求１７０は典型的には、ローカルプロセッサ１２２Ａ及び装置１１０ｂを識別する情報を含むであろう。また要求１７０は、プロキシ装置１４５がリモートプロセッサ１５７からローカルプロセッサ１２２Ａにメッセージをルーティングするのを認可するＨＴＴＰヘッダのプロキシ情報も含む。その結果、リモートプロセッサ１５７は、要求１７１を送出することにより応答し、その応答を、プロキシ装置１４５がローカルプロセッサ１２２Ａにルーティングする。要求１７１は、要求１７０への有効な応答であることに留意されたい。

【００３１】要求１７１は、装置１１０ｂに対して、ローカルプロセッサ１２２Ａによって実行されるべき１つ或いは複数のコマンドを指示するメッセージである。例えば、コマンドは、装置１１０ｂが再度初期化されるべきであることを示すことができる。また要求１７１は、リモートプロセッサ１５７に情報を送出するよう、ローカルプロセッサ１２２Ａを指示することができる。例えば、サポートアプリケーション１６０は、ローカルプロセッサ１２２Ａ及び装置１１０ｂの構成に関する付加情報を必要とする場合もある。ローカルプロセッサ１２２Ａは、応答１７２において要求された情報を送出する。

【００３２】応答１７２は、プロキシ装置１４５がリモートプロセッサ１５７からローカルプロセッサ１２２Ａに別の「応答」メッセージをルーティングするのを認可するＨＴＴＰヘッダのプロキシ情報を含む。その後、リモートプロセッサ１５７は、要求１７３を送出し、その要求を、プロキシ装置１４５がローカルプロセッサ１２２Ａにルーティングする。要求１７３は、装置１１０ｂに対して実行されるべきコマンドを指示することができ、またローカルプロセッサ１２２Ａを指示して、リモートプロセッサ１５７にさらに情報を与えることができる。要求１７３がローカルプロセッサ１２２が付加情報を送出する指示を含む場合には、ローカルコンピュータは、応答１７４においてその付加情報を送出する。

【００３３】この要求及び応答のパターンは、図２の内容に則して上で説明したものと同様である。ローカルプロセッサ１２２Ａによって、リモートプロセッサ１５７に送出される各メッセージ（要求１７０及び応答１７２、１７４）は、プロキシ装置１４５がメッセージ（要求１７１及び１７３）をリモートプロセッサ１５７からローカルプロセッサ１２２Ａにルーティングするのを認可するＨＴＴＰヘッダのプロキシ情報を含む。それにより装置１１０ｂは、リモートプロセッサ１５７から間接的に制御される。

【００３４】図４は、本発明による、全体的に参照番号２００によって示される装置管理プロセスの論理ステップを示す。上記のように、装置管理プロセス２００は、利用者によって起動される通信開始コマンド１３０、Ｅメール通信開始コマンド１４０或いは装置によって起動される通信開始コマンド１１３によって開始することができる。それぞれの場合に、装置管理プロセス２００は、ステップ２１０で開始し、ステップ２１５に進む。

【００３５】ステップ２１５では、ローカルプロセッサがリモートプロセッサにメッセージを送出し、またプロキシ装置がリモートプロセッサからローカルプロセッサにメッセージをルーティングするのを認可する。ローカルプロセッサからのメッセージは、ローカルプロセッサとリモートプロセッサとの間で通信を開始することを意図しており、典型的には、ローカルプロセッサ及び管理されるべき装置に関する構成情報を含む。

【００３６】ステップ２２０では、ローカルプロセッサはリモートプロセッサからメッセージを受信する。リモートプロセッサからのメッセージは、ローカルプロセッサによって実行されるべき１つ或いは複数のコマンドを指示する。

【００３７】ステップ２２５では、ローカルプロセッサは、ステップ２２０においてリモートプロセッサからのメッセージにおいて指示されたコマンドを実行する。例

えば、そのコマンドは、特定の装置の構成状態を読み出すことを要求したり、或いは装置を再度初期化するように能動的な動作を実行することを要求する場合もある。

【００３８】ステップ２３０では、ローカルプロセッサはさらにリモートプロセッサからのメッセージを評価し、リモートプロセッサに別のメッセージを送出するよう、リモートプロセッサがローカルプロセッサに要求しているか否かを判定する。例えば、リモートプロセッサからの以前のメッセージによって、装置の較正が開始されていると、リモートプロセッサは、ここで、較正が成功したか否かを判定するために、あるフィードバック情報を必要とする。

【００３９】ステップ２３０の間に行われる判定によって、リモートプロセッサは、ローカルプロセッサとのメッセージ交換を継続するか否かを制御できるようになる。プロキシ装置は、認可を受けた場合にのみ、メッセージをリモートプロセッサからローカルプロセッサにルーティングし、またその認可はメッセージ毎に必要になることを思い起こされたい。従って、リモートプロセッサからローカルプロセッサに送出される全てのメッセージの前に、ローカルプロセッサからプロキシ装置に対して認可が行われなければならない。リモートプロセッサがローカルプロセッサとの通信の保持を望む場合には、ローカルプロセッサへの各メッセージにおいて、リモートプロセッサは、ローカルプロセッサがリモートプロセッサに対して別のメッセージを送出するように指示しなければならない。

【００４０】リモートプロセッサからのメッセージが、ローカルプロセッサが別のメッセージを送出しなければならないことを示す場合には、そのプロセスはステップ２３５に進み、そうでない場合には、そのプロセスはステップ２５０に進む。

【００４１】ステップ２３５では、ローカルプロセッサは、次のメッセージをリモートプロセッサに送出し、またプロキシ装置が次のメッセージをリモートプロセッサからローカルプロセッサにルーティングするのを認可する。

【００４２】ステップ２４０では、ローカルプロセッサは、リモートプロセッサから次のメッセージを受信する。このリモートプロセッサからのメッセージは、ローカルプロセッサによって実行するべき１つ或いは複数のコマンドを指示する。

【００４３】ステップ２４５では、ローカルプロセッサは、ステップ２４０においてリモートプロセッサからのメッセージで指示されたコマンドを実行する。その後そのプロセスは、ステップ２３０に戻って繰り返される。

【００４４】ステップ２５０において、そのプロセスは終了する。

【００４５】上記のように、リバーストンネリングプロトコルは、ウエブブラウザによって、ファイヤウォールで保護されたウエブサイトを見るための簡単な機構を提供する。それは、ファイヤウォールが通過を許可する形態でウエブトラフィック要求及び応答を送信するシステムを実現するプロトコルである。上述の各実施形態では、ウエブサイト上で動作するアプリケーションは、トンネリングプロトコルを組み込むために変更される必要があった。多数のアプリケーションを変更するのを避けるために、図５は、個別のプロキシ装置を用いてファイヤウォールへのインターフェースを提供する、本発明の実施形態を示す。サーバ、ブラウザ、及び他のウエブサイト上で動作するアプリケーションがそのプロトコルを実施する代りに、これらのプロキシ装置がリバースＨＴＴＰ通信プロトコルを実施する。

【００４６】以下の記載からわかるように、図５の実施形態によって、ファイヤウォール内のエンティティは、ファイヤウォール外部のエンティティにアクセスを提供できるようになる。さらに、ファイヤウォール内部のエンティティは、リバースｈｔｔｐプロトコルセッションを何時でも終了し、ファイヤウォールの外部のウエブブラウザが、ファイヤウォール内部の装置にアクセスするのを防ぐことができる。

【００４７】コンピュータシステム３００は、ファイヤウォール３０５の内側３０２とファイヤウォール３０５の外側３０４との間に介在するファイヤウォール３０５を備える。内側３０２は、ウエブサーバ３０８Ｉと、ブラウザ３１４Ｉと、アプリケーション３１６Ｉとに接続されるプロキシエージェント３０６を備える。同様に、外側３０４は、ウエブサーバ３０８Ｅと、ブラウザ３１４Ｅと、アプリケーション３１６Ｅとに接続されるリバースプロキシ３１２を備える。内側３０２では、ファイヤウォール３０５は、プロキシエージェント３０６に接続され、外側３０４では、ファイヤウォール３０５は、インターネットのようなコンピュータネットワーク３０１を介してリバースプロキシ３１２に接続される。ファイヤウォール３０５によって、内側３０２の装置は、外側３０４の装置から発信される不要な通信から保護される。

【００４８】リバースプロキシエージェント３０６は、ファイヤウォール３０５と１つ或いは複数のウエブサーバ３０８Ｉとの間のインターフェースを形成する。各ウエブサーバ３０８Ｉは、１つ或いは複数のパーソナルコンピュータ（ＰＣ）３１０Ｉと通信を行う。各ＰＣ３１０Ｉは、ＨＴＴＰプロトコルに準拠する通信プログラムを組み込んでいる。プロキシエージェント３０６は、各ウエブサーバ３０８Ｉとファイヤウォール３０５とのインターフェースを形成する役割を担う。リバースプロキシエージェント３０６（以下、「エージェント」）は、ウエブサーバ３０８Ｉから受信する要求に応じて、ファイヤウォールを介して、ファイヤウォール３０５の外側３０４に配置されるリバースプロキシ装置３１２との接

続を開始する。この接続は、利用者が接続を閉じるまで、開いたままである。

【００４９】エージェント３０６の別の機能は、接続を介して外部装置から受信したブラウザ要求を抽出し、その要求を、適当なウエブサーバ３０８Ｉに転送することである。例えば、エージェント３０６は、ファイヤウォール３０５の外側３０４に位置するブラウザ３１４Ｅの代わりに、ウエブサーバ３０８Ｉへの要求を行う。エージェント３０６の別の機能は、ブラウザ３１４Ｅからの次の応答がファイヤウォール３０５によって確実に渡されるように、ウエブサーバ３０８Ｉから受信した応答を要求として符号化することである。

【００５０】リバースプロキシ３１２はまた、１つ以上のブラウザ３１４Ｅから受信した要求を、ファイヤウォール３０５によって遮断されることになる要求としてではなく応答としてファイヤウォール３０５によって認識されるコードによって「包む（wrap）」よう機能する。またリバースプロキシ３１２は、それぞれ接続の状態を保持し、エージェント３０６のような、どのエージェントが、プロキシとの接続を開始しているかを記憶し、ウエブサーバ３０８Ｉのような、どのサーバがアクセス可能であるかを認識する。同様に、リバースプロキシ３１２は、ブラウザ３１４Eのような、どのブラウザがプロキシとの接続を開いているかを記憶する。リバースプロキシ３１２は、エージェント３０６と同様にして、ブラウザ３１４Ｅから受信した要求を応答に変換し、エージェント３０６が、リバースプロキシ３１２から受信した応答を、その後、指示されたウエブサーバ３０８Ｉにディスパッチされる要求に変換するリバース機能を実行する。リバース方向では、エージェント３０６は、ウエブサーバ３０８Ｉから受信した応答を要求に変換し、その要求をファイヤウォール３０５を介してリバースプロキシサーバ３１２にディスパッチする。要求を受信すると、リバースプロキシ３１２は「包みを解いて」に、応答を適当なブラウザ３１４Ｅにディスパッチする。

【００５１】このようにして、ファイヤウォール３０５の保護機能は、エージェント３０６及びリバースプロキシ３１２の包み込み動作によってバイパスされる。接続を確立する初期要求を除いて、エージェント３０６は、内側３０２から受信した応答を要求のように見せるとともに、ファイヤウォール３０５から受信した応答を要求に変換する。同様に、リバースプロキシ３１２は、ファイヤウォール３０５から受信した要求を、要求を出しているブラウザ３１４Ｅにディスパッチするための応答に変換するとともに、ブラウザ３１４Ｅから受信した要求を応答のように見せる。

【００５２】内側或いは外側のような構成要素の呼び方は、単なる１つの見方にすぎないことに留意されたい。また通信は、ウエブサーバ３０８Ｅに接続されるＰＣ３１０ＥとブラウザＩとの間にも確立できる。そのような場合には、ＰＣ３１０Ｅ、ウエブサーバ３０８Ｅ及びブラウザ３１４Ｉの機能は、それぞれ上記のようなＰＣ３１０Ｉ、ウエブサーバ３０８Ｉ及びブラウザ３１４Ｅの機能と同様であり、エージェント３０６及びリバースプロキシ３１２の機能的な役割は逆になる。

【００５３】リバースプロキシ３１２及びエージェント３０６の規定によって、ブラウザ３１４Ｉ、３１４Ｅ及びウエブサーバ３０８Ｉ、３０８Ｅは、リバーストンネリング手順を全く知らなくても済むようになる。またその手順は、それぞれエージェント３０６及びリバースプロキシ３１２とのインターフェースを直接形成する３１６Ｉ及び３１６Ｅのようなアプリケーションに対して透過性がある。従って、本発明は、アプリケーション３１６Ｉ、３１６Ｅと、ＰＣ３１０Ｉ、３１０Ｅ上で動作するアプリケーションと、ウエブサーバ３０８Ｉ、３０８Ｅと、ブラウザ３１４Ｉ、３１４Ｅに関して、コードの変更或いは追加の修正を行うことなく、実施される。エージェント３０６及びリバースプロキシ３１２は、完全にソフトウエアで実施し、ファイヤウォール３０５と同様の機器上に常駐させるか、個別の機器に常駐させることもできる。

【００５４】上記の説明は、本発明の例にすぎないことを理解されたい。当業者は、本発明から逸脱することなく、種々の変更形態及び変形形態を考案することができるであろう。例えば、管理されている装置は、任意のコンピュータ周辺機器、別のコンピュータ、或いはローカルプロセッサそのものとすることができる。また、ファイヤウォール或いはプロキシ装置を備えないシステムの場合には、プロキシ装置がメッセージをローカルプロセッサにルーティングするのを認可するステップを単に削除するだけで、その手順を適用することができる。さらに、本発明を実行するために必要とされるプロセスは、ローカルコンピュータのメモリに予めロードされているものとして示されるが、後にローカルコンピュータにロードするために、図２のデータメモリ１１５及び図３のデータメモリ１１５Ａのような記憶媒体上で構成されることもできる。従って、本発明は、添付の請求の範囲の中に入る全ての別形態、変更形態及び変形形態を含むつもりである。

【００５５】以上、本発明の実施例について詳述したが、以下、本発明の各実施態様の例を示す。

【００５６】〔実施態様１〕リモートプロセッサ（３１４Ｅ）が、リバースプロキシ装置（３１２）と、コンピュータネットワーク（３０１）と、ファイヤウォール（３０５）と、プロキシエージェント装置（３０６）とを介してローカルプロセッサ（３０８Ｉ）に結合される場合に、前記リモートプロセッサ（３１４Ｅ）が前記ローカルプロセッサ（３０８Ｉ）と通信できるようにするトンネリング動作を可能にするための方法であって、ローカル要求メッセージを前記プロキシエージェント装置（３

０６）にディスパッチさせて前記リモートプロセッサ（３１４Ｅ）との通信チャネルを確立するよう、前記ローカルプロセッサ（３０８Ｉ）を制御するステップであって、前記プロキシエージェント装置（３０６）は前記ファイヤウォール（３０５）と前記ネットワーク（３０１）とを介して前記ローカル要求メッセージを前記リバースプロキシ装置（３１２）にディスパッチし、前記ファイヤウォール（３０５）は前記プロキシエージェント装置（３０６）によって前記ローカル要求メッセージに対するリモート応答メッセージを受信することができるようになされる、制御ステップと、前記通信チャネルの確立に基づき、前記リモートプロセッサ（３１４Ｅ）が前記リバースプロキシ装置（３１２）にリモート要求メッセージを送出するのを可能にし、次に、前記リバースプロキシ装置（３１２）が、前記リモート要求メッセージを中に含んだリモート応答メッセージをディスパッチするのを可能にするステップと、前記ファイヤウォール（３０５）を介して前記プロキシエージェント装置（３０６）が前記リモート応答メッセージを受信したときに、前記リモート要求メッセージを抽出して該リモート要求メッセージを前記ローカルプロセッサ（３０８Ｉ）にディスパッチするよう前記プロキシエージェント装置（３０６）を制御するステップと、を備えて成り、前記プロキシエージェント装置（３０６）及び前記リバースプロキシ装置（３１２）が、前記ローカルプロセッサ（３０８Ｉ）または前記リモートプロセッサ（３１４Ｅ）のいずれかにおける通信アプリケーションを変更することなく、前記トンネリング動作を可能にすることを特徴とする方法。

【００５７】〔実施態様２〕ローカル応答メッセージをローカル要求メッセージに組み込み、前記ローカル要求メッセージを前記ファイヤウォール（３０５）と、前記ネットワーク（３１０）と、前記リバースプロキシ装置（３１２）とを介して前記リモートプロセッサ（３１４Ｅ）にディスパッチすることにより、前記リモート要求メッセージに対する前記ローカルプロセッサ（３０８Ｉ）からの前記ローカル応答メッセージの受信に応答するよう前記プロキシエージェント装置（３０６）を制御するステップであって、前記ファイヤウォール（３０５）は前記ローカル要求メッセージに対するリモート応答メッセージを受信することができるよう前記プロキシエージェント装置（３０６）によってなされる、ステップ、をさらに備えて成ることを特徴とする、実施態様１に記載の方法。

【００５８】〔実施態様３〕前記ファイヤウォール（３０５）を介して前記リバースプロキシ装置（３１２）が前記ローカル要求メッセージを受信したときに、前記ローカル応答メッセージを抽出して該ローカル応答メッセージを前記リモートプロセッサ（３１４Ｅ）にディスパッチするよう前記リバースプロキシ装置（３１２）を制御するステップ、をさらに備えて成ることを特徴とする、実施態様２に記載の方法。

【００５９】〔実施態様４〕前記コンピュータネットワーク（３０１）は、インターネットであり、前記プロキシエージェント装置（３０６）と前記リバースプロキシ装置（３１２）との間でディスパッチされるメッセージは、ＨＴＴＰフォーマットで構成されることを特徴とする、実施態様１に記載の方法。

【００６０】〔実施態様５〕リモートプロセッサ（３１４Ｅ）が、コンピュータネットワーク（３０１）と、ファイヤウォール（３０５）とを介して、ローカルプロセッサ（３０８Ｉ）に結合される場合に、前記リモートプロセッサ（３１４Ｅ）が前記ローカルプロセッサ（３０８Ｉ）と通信できるようにするトンネリング動作を可能にするシステムであって、前記ローカルプロセッサ（３０８Ｉ）からのローカル要求に応答して前記ファイヤウォール（３０５）を介してローカル要求メッセージをディスパッチすることにより、前記リモートプロセッサ（３１４Ｅ）との通信チャネルを確立するプロキシエージェント手段（３０６）であって、前記ファイヤウォール（３０５）は前記ローカル要求メッセージに対するリモート応答メッセージを受信することができるよう前記プロキシエージェント手段（３０６）によってなされる、プロキシエージェント手段と、前記ローカル要求メッセージの受信と、前記リモートプロセッサ（３１４Ｅ）からのリモート要求メッセージの受信とに応答して、前記リモート要求メッセージを中に含んだリモート応答メッセージをディスパッチするリバースプロキシ手段（３１２）と、を備えて成り、前記ファイヤウォール（３０５）を介して前記プロキシエージェント手段（３０６）が前記リモート応答メッセージを受信したときに、前記プロキシエージェント手段（３０６）は、前記リモート要求メッセージを抽出して該前記リモート要求メッセージを前記ローカルプロセッサ（３０８Ｉ）にディスパッチし、それにより、前記プロキシエージェント手段（３０６）及び前記リバースプロキシ手段（３１２）が、前記ローカルプロセッサ（３０８Ｉ）または前記リモートプロセッサ（３１４Ｅ）のいずれかにおける通信アプリケーションを変更することなく、前記トンネリング動作を可能にすることを特徴とするシステム。

【００６１】〔実施態様６〕前記ローカル応答メッセージをローカル要求メッセージに組み込み、前記ローカル要求メッセージを前記ファイヤウォール（３０５）と、前記ネットワーク（３１０）とを介して、前記リバースプロキシ手段（３１２）にディスパッチすることにより、前記プロキシエージェント手段（３０６）は前記リモート要求メッセージに対する前記ローカルプロセッサ（３０８Ｉ）からの前記ローカル応答メッセージの受信に応答し、前記ファイヤウォール（３０５）は前記ローカル要求メッセージに対するリモート応答メッセージを受信

15

することができるよう前記プロキシエージェント手段（３０６）によってなされることを特徴とする、実施態様５に記載のシステム。

【００６２】〔実施態様７〕前記リバースプロキシ手段（３１２）が、前記ファイヤウォール（３０５）を介して前記ローカル要求メッセージを受信したとき、前記リバースプロキシ手段（３１２）は、前記ローカル応答メッセージを抽出して該ローカル応答メッセージを前記リモートプロセッサ（３１４Ｅ）にディスパッチすることを特徴とする、実施態様６に記載のシステム。

【００６３】〔実施態様８〕前記コンピュータネットワーク（３０１）はインターネットであり、前記プロキシエージェント手段（３０６）と前記リバースプロキシ手段（３１２）との間でディスパッチされるメッセージは、ＨＴＴＰフォーマットで構成されることを特徴とする、実施態様５記載のシステム。

【００６４】

【発明の効果】以上説明したように、本発明を用いることにより、インターネットとローカルコンピュータシステムとの間にファイヤウォールが介在する通信において、ローカルコンピュータシステム或いはリモートコンピュータシステムのいずれかにおいて動作するアプリケーションを変更せずに、リモートコンピュータシステムがインターネットを介してローカルコンピュータシステムにアクセスすることができる。

【図面の簡単な説明】

【図１】従来技術による、プロキシ装置を介してインターネットに接続されるローカルコンピュータを備えるコンピュータシステムのブロック図である。

【図２】特に本発明を実行するように構成されたコンピュータシステムのブロック図である。

【図３】本発明を実行するためのコンピュータシステムの別の実施形態のブロック図である。

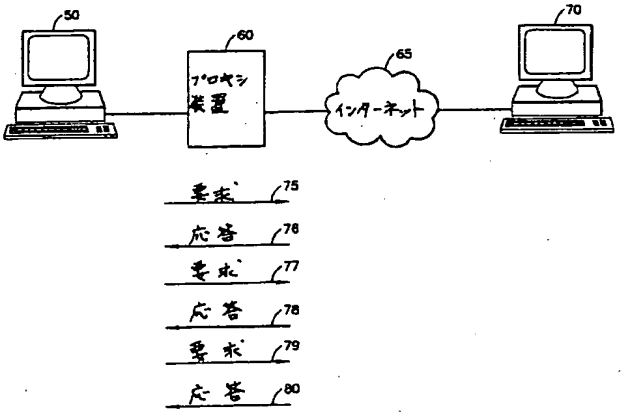
【図４】本発明の方法を示す流れ図である。

【図５】本発明の別の実施形態のブロック図である。

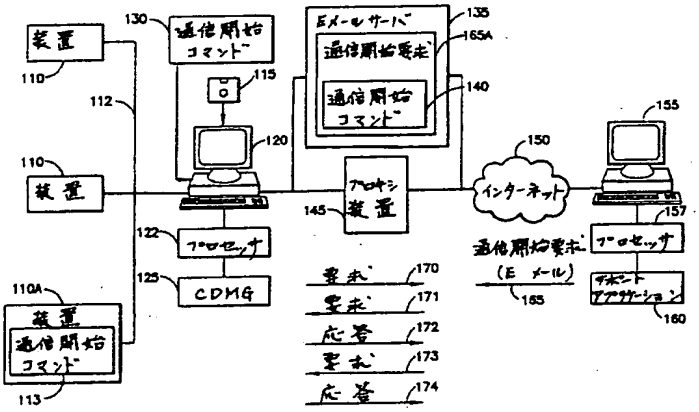
【符号の説明】

３０１：コンピュータネットワーク
３０５：ファイヤウォール
３０６：プロキシエージェント装置
３０８Ｉ：ローカルプロセッサ
３１２：リバースプロキシ装置
３１４Ｅ：リモートプロセッサ

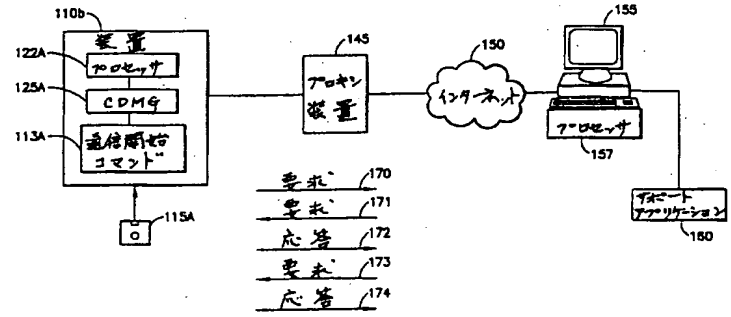
【図１】



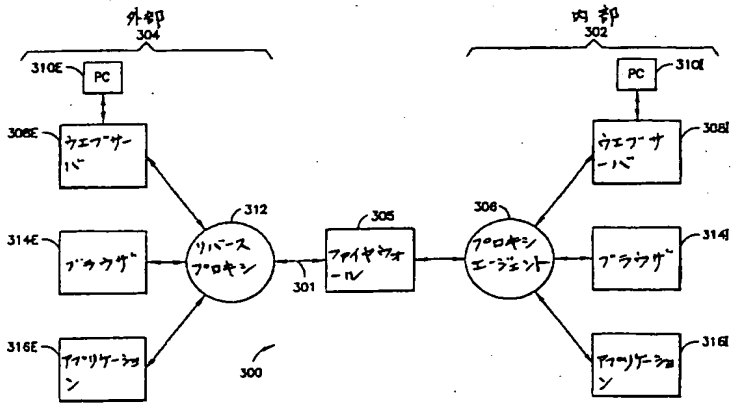
【図２】


装置
110
通信開始コマンド
130
112
115
120
Eメールサーバ
135
通信開始要求
165A
通信開始コマンド
140
155
150
インターネット
プロキシ装置
145
プロセッサ
157
通信開始要求
(Eメール)
165
ディジタルアプリケーション
160
122
プロセッサ
125
CDMA
110A
装置
通信開始コマンド
113
要求 170
要求 171
応答 172
要求 173
応答 174

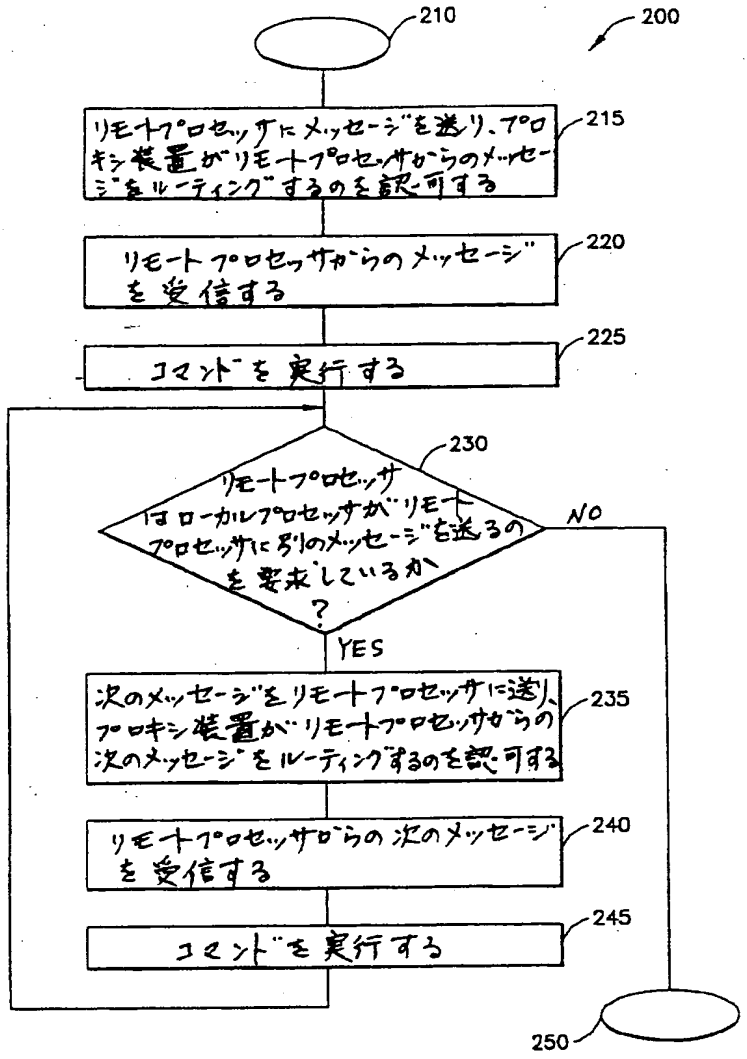
【図３】


110b
装置
122A
プロセッサ
125A
CDMA
113A
通信開始コマンド
115A
145
プロキシ装置
150
インターネット
155
プロセッサ
157
ディジタルアプリケーション
160
要求 170
要求 171
応答 172
要求 173
応答 174

【図５】


外部
304
内部
302
310E
PC
310I
PC
308E
ウェブサーバ
308I
ウェブサーバ
312
リバースプロキシ
305
ファイヤウォール
306
プロキシエージェント
314E
ブラウザ
314I
ブラウザ
316E
アプリケーション
316I
アプリケーション
301
300

【図４】



フロントページの続き

(72)発明者 ジェイムス・クラフ
アメリカ合衆国アイダホ州メリディアン
イースト・ウェイクリー・ストリート
465

(72)発明者 ディーン・エス・ネルソン
アメリカ合衆国アイダホ州メリディアン
ウエスト・ブルー・クリーク ドライブ
4049